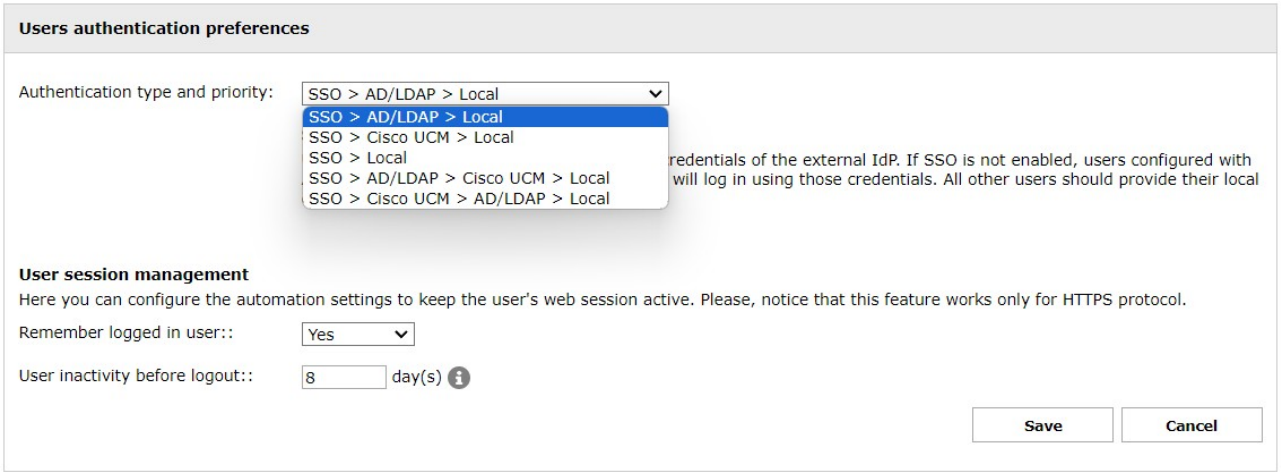
imagicle

Users Authentication Settings

This important setting dictates the authority in charge of authenticate users upon accessing Imagicle web portal, gadgets and Attendant Console. Within same page, you can also setup the https session expiration timeout for Imagicle web portal and gadgets.

This setting is available from Imagicle UCX Suite web portal: Admin â System Parameters â Users authentication settings.

Users authentication preferences



As you can see in above screenshot sample, it includes several different authentication authorities. Please configure the one corresponding to your synchronization source:

- **SSO > AD/LDAP > Local**: Choose this option when you import users from Active Directory, from Azure AD, from a generic LDAP server or from Imagicle LDAP Module.
- **SSO > Cisco UCM > Local**: Choose this option while importing users from Cisco UCM (via AXL) or from Cisco Webex Control Hub.
- **SSO > Local**: This is the local authentication, leveraging a local username and password assigned to each Imagicle user and stored into Imagicle SQL Server instance.
- **SSO > AD/LDAP > Cisco UCM > Local**: Choose this option to authenticate users against Active Directory or generic LDAP. If AD/LDAP username is missing and PBX Username is configured, users are authenticated against Cisco UCM.
- **SSO > Cisco UCM > AD/LDAP > Local**: Choose this option to authenticate users against Cisco UCM. If PBX Username is missing and AD/LDAP username is configured, users are authenticated against Active Directory or generic LDAP.

Please note that all above options include SSO authentication against a configured Identity Provider. If SSO is not used, and relevant User's field is left empty, then authentication is skip to next listed option.

All above choices include "Local" as last authentication option, meaning UCX Suite authentication leveraging a local username and password assigned to each Imagicle user and stored into Imagicle SQL Server instance.

User session management

This setting allows to enable a persistent active web session for users leveraging Imagicle web portal and/or Imagicle gadgets.

If this feature is enabled, by configuring "Remember logged in user" to Yes, users can shut down own workstations or close the web browser without loosing entered login credentials. Next time they access to Imagicle web portal or gadget within configured inactivity period, they are redirected to web portal's home page or gadgets' main pages.

The feature is enabled by default, with an inactivity timeout of 8 days. You an increase this parameter up to 30 days.